REMARKS

Claims 1-35, 69-79, 88, 89-91 are pending. Claims 1, 69, 88, and 89 are in independent form.

Status of the Claims

In the Office Action mailed October 22, 2009, claims 1-35, 69-79, and 88-91 were recognized and reciting allowable subject matter. *See Office Action mailed October 22, 2009*, p. 4, para. 5. However in the same Office action, the Examiner later stated that "Applicant's arguments with respect to prior art rejection of claims 1 - 35 have been fully considered but they are not persuasive… Examiner maintains previous Examiner's prior art rejection (mailed 8/12/2009) for Claim 1 and all of the dependent claims of 1, by the virtue of their dependency and requests to amend the [i]ndependent claim 1 similar to the allowed subject matter that is detailed in item #5." *See Office Action mailed October 22, 2009*, p. 2, para. 2. Subsequently, in paragraph 3 of the same Office action, the Examiner states that "Applicant's arguments with respect to the rejection(s) of claim(s) 69 - 79 and 81 – 91 under prior art rejection have been fully considered and are persuasive." *See Office Action mailed October 22, 2009*, p. 2, para. 3.

Applicant respectfully requests that the status of the claims be clarified. In light of the fact that no ground for rejection of claims 69-79, 88, and 89-91 has been set forth, Applicant will assume that these claims do indeed stand allowed except for the double patenting rejections discussed below.

Applicant acknowledges the indication of allowable subject matter with appreciation.

Rejections under 35 U.S.C. § 103(a)

Claim 1 may be rejected under 35 U.S.C. § 103(a) as obvious over U.S. Patent No. 6,477,651 to Teal et al. (hereinafter "Teal") and U.S. Patent No. 6,988,208 to Hrabik et al. (hereinafter "Hrabik").

As shown above, claim 1 has been amended to clarify that the common content is sent to one or more of a signature blocker and a signature manager for use as a new signature in identifying the previously unknown intrusive network attack. As discussed previously, Teal and Hrabik both describe systems that necessarily operate with old signatures of known network attacks. Accordingly, even if Teal and Hrabik were combined, one of ordinary skill would not arrive at the recited subject matter. Claim 1 is thus not obvious over Teal and Hrabik. Applicant respectfully requests that any obviousness rejection of claim 1 and its dependencies be withdrawn.

Double Patenting Rejections

Claim 1 and its dependencies were rejected under the judicially-created doctrine of obviousness-type double patenting over claims 1-7, 9-20, and 22-26 of U.S. Patent Application No. 11/271,133 to Singh and Varghese (hereinafter "the '133 application"). The '133 application was filed on November 9, 2005, i.e., after the April 8, 2004 filing date of the present application. The '133 application is still pending, although a Notice of Allowance was mailed on October 07, 2009.

As a threshold matter, it appears that the present double patenting rejections are provisional rejections, since the '133 application is not a patent but rather an application. *See, e.g.,* M.P.E.P. § 804(I)(B), Chart I-A and I-B. Please note that no corresponding provisional double patenting rejections have been made in the '133 application.

Further, the Office action is understood to contend that the "obviousness-type double patenting rejections" are appropriate since "[c]laims of the instant application are anticipated by patent claims in that the patent claims contains all the limitations of the instant application." *See, e.g., Office Action mailed October 22, 2009*, p. 4 (emphasis added).

Regardless whether the claims in the present application are allegedly anticipated by or obvious over the claims in the '133 application, Applicant respectfully disagrees.

As a threshold matter, if the rejections are indeed potential obviousness-type double patenting rejections, the rejections do not set forth the basis on which they are made. In particular, M.P.E.P. § 804(II)(B)(1) states that:

> "Any obviousness-type double patenting rejection should make clear:
> (A) The differences between the inventions defined by the conflicting claims — a claim in the patent compared to a claim in the application; and
> (B) The reasons why a person of ordinary skill in the art would conclude that the invention defined in the claim at issue is anticipated by, or would have been an obvious variation of, the invention defined in a claim in the patent." See M.P.E.P. § 804(II)(B)(1) (emphasis added). See also 35 U.S.C. § 132 and 37 C.F.R. § 1.104(2) (requiring that the reasons for any adverse action be stated in an Office action).

Accordingly, if the rejections are indeed potential obviousness-type double patenting rejections, the present double patenting rejections are facially deficient and applicant respectfully requests that they either be withdrawn or that the reasoning behind the rejections be stated.

Further, it appears that this failure relates to the merits of the double patenting rejections. For the sake of convenience, claim 1 in the present application is presented in dual column format adjacent claim 1 in the '133 application as an illustrative example.

THE PRESENT APPLICATION

1. A machine-implemented method for automatically identifying new signatures to use in identifying a previously unknown intrusive network attack, comprising:

　　obtaining a collection of data items to be analyzed to identify the network attack, wherein said data items are parts of messages that were sent over a data network;

　　reducing said data items in said collection to reduce said data collection to a reduced data collection of reduced data items, wherein the reduced data items in the reduced data collection have a smaller size and a constant predetermined relation with data items in the data collection and at least some of the data items in the data collection that differ are reduced to the same reduced data item;

　　analyzing a plurality of said reduced data items to detect common elements in the plurality of said reduced data items, said analyzing identifying common content indicative of the previously unknown network attack; and

　　sending the common content to one or more of a signature blocker and a signature manager.

THE '133 APPLICATION

1. A method for detecting malicious attacks, the method comprising:

　　obtaining routing information from a packet communicated via a network, the routing information including a source address and a destination address;

　　maintaining a count of packets associated with a device associated with the routing information;

　　identifying the device as a potentially malicious device when the count exceeds a threshold;

　　mapping the source address into a source infected set and mapping the destination address into a destination infected set; and

　　selectively categorizing the source device associated with the packet as a suspicious device.

As can be seen, claim 1 in the present application relates to a method for automatically identifying new signatures to use in identifying a previously unknown intrusive network attack. In contrast, claim 1 the '133 application relates to categorizing a source device as a suspicious device. Claim 1 in the present application is thus neither anticipated by nor obvious over claim 1 the '133 application.

Further, the method by which new signatures are identified in claim 1 of the present application is different from the method by which a source device is categorized as a suspicious device in claim 1 in the '133 application. For example, the identification of new signatures includes reducing data items to a reduced data collection, analyzing reduced data items to detect common elements, and sending common content to one or more of a signature blocker and a signature manager.

These and other features in claim 1 of the present application are neither described nor suggested by the categorization of a source device as a suspicious device in claim 1 the '133 application. As discussed in M.P.E.P. § 804(II)(B)(1), the analysis employed in an obviousness-type double patenting determination parallels the guidelines for a 35 U.S.C. 103(a) rejection. Applicant respectfully requests that

the reasoning behind any conclusion that claim 1 or its dependencies in the present application are obvious variants of the claims the '133 application be stated.

Accordingly, the (provisional)(obviousness-type) double patenting rejections of claim 1 and its dependencies in the present application are improper and Applicant requests that they be withdrawn.

Claims 69, 88, and 89 and their dependencies were also (provisionally) rejected under the judicially-created doctrine of (obviousness-type) double patenting over claims 1-7, 9-20, and 22-26 of the '133 application.

These rejections are deficient on several bases. To begin with, it is self-evident that the claims do not anticipate one another and the grounds of the obviousness-type double patenting rejections of these claims are not stated. Hence, the rejections are improper under 35 U.S.C. § 132.

Further, claims 69, 88, and 89 relate to methods for automatically identifying new signatures to use in identifying a previously unknown intrusive network attack. In contrast, claim 1 the '133 application relates to categorizing a source device as a suspicious device. The methods by which new signatures are identified in claims 69, 88, and 89 of the present application

differ from the method by which a source device is categorized as a suspicious device in claim 1 in the '133 application on several grounds, as is apparent from the claims.

Accordingly, the (provisional) (obviousness-type) double patenting rejections of claims 69, 88, and 89 and their dependencies in the present application are improper. Applicant requests that they be withdrawn.

Claim 1 and its dependencies were rejected under the judicially-created doctrine of obviousness-type double patenting over claims 1-20 of U.S. Patent No. 7,535,909 to Singh and Varghese (hereinafter "the '909 patent"). The '909 patent was filed on November 9, 2005, i.e., after the April 8, 2004 filing date of the present application. The '909 patent issued on May 19, 2009.

No corresponding provisional double patenting rejections were made in the '909 patent. Further, as best understood, the "obviousness-type double patenting rejections" are based on the contention that "[c]laims of the instant application are anticipated by patent claims in that the patent claims contains all the limitations of the instant application."

Applicant respectfully disagrees regardless of whether the rejections are obviousness-type double patenting rejections or not. However, as a threshold matter, if the rejections are indeed potential obviousness-type double patenting rejections, the present rejections do not set forth the basis on which they are made. As discussed above, M.P.E.P. § 804(II)(B)(1) states that both the differences between the inventions defined by the conflicting claims and the reasons why a person of ordinary skill in the art would conclude that the invention defined in the claims are obvious variants should be made clear. *See also* 35 U.S.C. § 132 and 37 C.F.R. § 1.104(2).

Accordingly, the present obviousness-type) double patenting rejections are facially deficient. Applicant respectfully requests that either the rejections be withdrawn or that the reasoning behind the rejections be stated.

Further, it appears that this failure relates to the merits of the (obviousness-type) double patenting rejections themselves. For the sake of convenience, claim 1 in the present application is presented in dual column format adjacent claim 1 in the '909 patent is presented as an illustrative example.

THE PRESENT APPLICATION

1. A machine-implemented method for automatically identifying new signatures to use in identifying a previously unknown intrusive network attack, comprising:

obtaining a collection of data items to be analyzed to identify the network attack, wherein said data items are parts of messages that were sent over a data network;

reducing said data items in said collection to reduce said data collection to a reduced data collection of reduced data items, wherein the reduced data items in the reduced data collection have a smaller size and a constant predetermined relation with data items in the data collection and at least some of the data items in the data collection that differ are reduced to the same reduced data item;

analyzing a plurality of said reduced data items to detect common elements in the plurality of said reduced data items, said analyzing identifying common content indicative of the previously unknown network attack; and

sending the common content to one or more of a signature blocker and a signature manager.

THE '909 PATENT

1. A method to process packets in a network, the method comprising:

receiving a packet;

determining a length K of the packet;

if the length of the packet is less than a reference length M, performing no analysis on the packet;

if the packet length K is not less than M, determining if the packet length K is greater than a reference window size W_{Ref}

wherein if the packet length is greater than or equal to W_{Ref}; then a window size W for processing of the packets is set equal to W_{Ref}; and

if the packet length is less than W_{Ref}, then a window size W for processing of the packets is set equal to the packet size K; and

processing the packets by a signature processing engine using the window size W.

As can be seen, claim 1 in the present application relates to a method for automatically identifying new signatures to use in identifying a previously unknown intrusive network attack. In contrast, claim 1 the '909 patent is understood to relates to the use of signatures by, e.g., a signature processing engine. Claim 1 in the present application is thus not anticipated by nor obvious over claim 1 the '909 patent.

Further, the method by which new signatures are identified in claim 1 of the present application is different from the method by which signatures are used in claim 1 in the '909 patent. For example, claim 1 of the present application recites that data items are reduced to a reduced data collection of reduced data items, the reduced data items are analyzed, and common content is sent to one or more of a signature blocker and a signature manager. Claim 1 in the '909 patent neither describes nor suggests these features.

Accordingly, the (obviousness-type) double patenting rejections of claim 1 and its dependencies in the present application are improper and Applicant requests that they be withdrawn.

Claims 69, 88, and 89 and their dependencies were also
rejected under the judicially-created doctrine of obviousness-
type double patenting over claims 1-20 of the '909 patent.

These rejections are deficient on several bases. To begin
with, it is self-evident that the claims do not anticipate one
another and the grounds of the obviousness-type double patenting
rejections of these claims are not stated. Hence, the
rejections are improper under 35 U.S.C. § 132.

Further, claims 69, 88, and 89 relate to methods for
automatically identifying new signatures to use in identifying a
previously unknown intrusive network attack. In contrast, claim
1 the '909 patent relates to the use of signatures.

Further, the methods by which new signatures are identified
in claims 69, 88, and 89 of the present application differ from
the method by signatures are used in claim 1 in the '909 patent
on several grounds, as is apparent from the claims.

Accordingly, the (obviousness-type) double patenting
rejections of claims 69, 88, and 89 and their dependencies in
the present application are improper. Applicant requests that
they be withdrawn.

It is believed that all of the pending claims have been addressed. However, the absence of a reply to a specific rejection, issue, or comment does not signify agreement with or concession of that rejection, issue, or comment. In addition, because the arguments made above may not be exhaustive, there may be reasons for patentability of any or all pending claims (or other claims) that have not been expressed. Finally, nothing in this paper should be construed as an intent to concede any issue with regard to any claim, except as specifically stated in this paper, and the amendment of any claim does not necessarily signify concession of unpatentability of the claim prior to its amendment.

Applicant asks that all claims be allowed. No fees are believed due at this time. Please apply any charges or credits, to Deposit Account No. 06-1050.

Respectfully submitted,

Date: November 30, 2009   /John F. Conroy, Reg. 45,485/
                                  John F. Conroy
                                  Reg. No. 45,485

Fish & Richardson P.C.
PTO Customer No. 20985
12390 El Camino Real
San Diego, California 92130
(858) 678-5070 telephone
(858) 678-5099 facsimile

JFC/jhg
14009833.doc